

What Is Claimed Is:

- 1 1. A method for providing identification authentication, comprising:
2 receiving an identification credential from an individual, including a
3 biometric data, wherein the identification credential is digitally signed with a
4 private key;
5 receiving a biometric sample from the individual;
6 validating the digital signature using a corresponding public key;
7 determining if a difference between the digitally signed biometric data and
8 the biometric data from the individual is below a predetermined threshold; and
9 providing the results of the determination to an interested party;
10 whereby the identity of the individual can be authenticated with reference
11 to the identification credential alone, without having to lookup information for the
12 individual in a database.
- 1 2. The method of claim 1, further comprising adjusting the
2 predetermined threshold in accordance with instructions received from a user.
- 1 3. The method of claim 1, wherein the identification credential can
2 include a name, a unique ID, a citizenship, an issue date, an expiration date, an
3 identifier for an issuing authority, the biometric data, and a digital photo..
- 1 4. The method of claim 1, wherein the biometric sample can include
2 one of, or a combination of, a fingerprint, a signature, an iris scan, a facial scan, a
3 voice pattern, a height, a weight, or a palm scan.

1 5. The method of claim 1, wherein the digitally signed biometric data
2 is contained in a magnetic stripe, a bar code, a smart card, a chip-card, or a non-
3 volatile memory, such as flash memory, located on or within the identification
4 credential.

1 6. The method of claim 1, wherein the digital signature is provided by
2 a central certification authority.

1 7. The method of claim 1, further comprising granting access to
2 resources based on the determination if the difference between the digitally signed
3 biometric data and the biometric data from the individual is below the
4 predetermined threshold.

1 8. A computer-readable storage medium storing instructions that
2 when executed by a computer cause the computer to perform a method for
3 providing identification authentication, the method comprising:
4 receiving an identification credential from an individual, including a
5 biometric data, wherein the identification credential is digitally signed with a
6 private key;
7 receiving a biometric sample from the individual;
8 validating the digital signature using a corresponding public key;
9 determining if a difference between the digitally signed biometric data and
10 the biometric data from the individual is below a predetermined threshold; and
11 providing the results of the determination to an interested party;
12 whereby the identity of the individual can be authenticated with reference
13 to the identification credential alone, without having to lookup information for the
14 individual in a database.

1 9. The computer-readable storage medium of claim 8, wherein the
2 method further comprises adjusting the predetermined threshold in accordance
3 with instructions received from a user.

1 10. The computer-readable storage medium of claim 8, wherein the
2 identification credential can include a name, a unique ID, a citizenship, an issue
3 date, an expiration date, an identifier for an issuing authority, the biometric data,
4 and a digital photo.

1 11. The computer-readable storage medium of claim 8, wherein the
2 biometric sample can include one of, or a combination of, a fingerprint, a
3 signature, an iris scan, a facial scan, a voice pattern, a height, a weight, or a palm
4 scan.

1 12. The computer-readable storage medium of claim 8, wherein the
2 digitally signed biometric data is contained in a magnetic stripe, a bar code, a
3 smart card, a chip-card, or a non-volatile memory, such as flash memory, located
4 on or within the identification credential.

1 13. The computer-readable storage medium of claim 8, wherein the
2 digital signature is provided by a central certification authority.

1 14. The computer-readable storage medium of claim 8, wherein the
2 method further comprises granting access to resources based on the determination
3 if the difference between the digitally signed biometric data and the biometric data
4 from the individual is below the predetermined threshold.

005437-012003

1 15. An apparatus for providing identification authentication,
2 comprising:
3 a receiving mechanism that is configured to receive an identification
4 credential from an individual, including a biometric data, wherein the
5 identification credential is digitally signed with a private key;
6 a sampling mechanism that is configured to receive a biometric sample
7 from the individual;
8 a validation mechanism that is configured to validate the digital signature
9 using a corresponding public key;
10 a determination mechanism that is configured to determine if a difference
11 between the digitally signed biometric data and the biometric data from the
12 individual is below a predetermined threshold; and
13 a feedback mechanism that is configured to provide the results of the
14 determination to an interested party;
15 whereby the identity of the individual can be authenticated with reference
16 to the identification credential alone, without having to lookup information for the
17 individual in a database.

1 16. The apparatus of claim 15, further comprising an adjustment
2 mechanism configured to adjust the predetermined threshold in accordance with
3 instructions received from a user.

1 17. The apparatus of claim 15, wherein the identification credential can
2 include a name, a unique ID, a citizenship, an issue date, an expiration date, an
3 identifier for an issuing authority, the biometric data, and a digital photo.

1 18. The apparatus of claim 15, wherein the biometric sample can
2 include one of, or a combination of, a fingerprint, a signature, an iris scan, a facial
3 scan, a voice pattern, a height, a weight, or a palm scan.

1 19. The apparatus of claim 15, wherein the digitally signed biometric
2 data is contained in a magnetic stripe, a bar code, a smart card, a chip-card, or a
3 non-volatile memory, such as flash memory, located on or within the
4 identification credential.

1 20. The apparatus of claim 15, wherein the digital signature is
2 provided by a central certification authority.

1 21. The apparatus of claim 15, further comprising a security
2 mechanism configured to grant access to resources based on the determination if
3 the difference between the digitally signed biometric data and the biometric data
4 from the individual is below the predetermined threshold.